2025 年 4 月 4 日

Babylon、Bitcoin ステーキングの仕組みと日本法

創・佐藤法律事務所
弁護士　斎藤　創

本稿では、Bitcoin(BTC)ステーキングの先駆的プロジェクトであり、現在の最大手と目される「Babylon」の仕組みと、それに関連する日本法上の論点について解説します。

これまで、ステーキングは主に Ethereum などの Proof of Stake(PoS)チェーン上で行われてきました。PoS におけるステーキングとは、ネットワーク上でトランザクションの検証等に参加することで、そのチェーンのセキュリティを高め、対価として報酬を得る仕組みです。

これに対し、Bitcoin は Proof of Work(PoW)を採用しているため、従来の意味でのステーキングによる収益機会は原則として存在しないと考えられてきました。BTC を活用した収益化手段としては、これまで、中央集権的な貸付サービスや、wBTC(Wrapped BTC)のようなトークン化ソリューションが主流でした。

Babylon は、このような BTC 活用の制約を克服し、BTC を用いたトラストレスなステーキングの実現を目指すプロジェクトであり、現在この分野において最も注目されているプロトコルの一つといえます。Babylon の仕組みを理解することは、グローバルな Web3 の潮流を読み解くうえでも有用であり、本稿では、その技術的構造と日本法上の課題について検討します。

なお、Bitcoin ステーキングの理解にあたっては、前提知識として PoS チェーンにおける基本的なステーキングの仕組み、LIDO 等によるリキッドステーキング、EigenLayer に代表されるリステーキングの概念について、一定の理解が望ましいと考えられます。これらに関しては、当事務所執筆の以下の記事もあわせてご参照ください。

(参考)POS チェーンのステーキングに関する当事務所の以前の Article

- ステーキングに関する法的論点の整理(2020.3.17)
- DeFi と法律 －LIDO やリキッドステーキングの仕組みと日本法(2023.10.17)
- EigenLayer などリステーキングの仕組みと日本法(2024.5.10)

I. 法律整理の纏め

(1) Babylon の仕組み自体は、資金決済法上のカストディ規制には該当しないと考えられます。

(2) 同様に、Babylon の仕組みは、金融商品取引法上のファンド規制(集団投資スキーム等)にも該当しないと解されます。

(3) もっとも、たとえばリキッドステーキング業者等が仮にユーザーの BTC 秘密鍵を預かるような場合には、当該業者が資金決済法上のカストディ規制等に該当する可能性もあるため、個別に法的検討を要します。

(4) 日本の暗号資産交換業者が、Babylon を通じた BTC ステーキングサービスを提供すること自体は、法的に許容されると考えられます。

(5) Babylon の仕組みにより付与される報酬が、当該業者にとって「取扱暗号資産」に該当しないアルトコインである場合、これをユーザーのためにカストディすることはできません。そのため、①ユーザーのアンホステッドウォレットに送付する、②当該アルトコインを DEX や海外の提携会社等で売却・交換し、BTC や日本円等でユーザーに報酬を支払う、等、対応を検討する必要があります。

II. Babylon の基本概要

1 Babylon の Bitcoin ステーキングとは

Bitcoin は PoW(Proof of Work)を採用しているため、Ethereum のように自らのネットワーク上でネイティブにステーキングを行う仕組みは存在しません。

Babylon はこの制約を乗り越え、Bitcoin を活用して他のネットワークのセキュリティを担保するという新たな仕組みを提供しています。主な特徴は以下のとおりです：

(1) Bitcoin のネットワーク自体を守るのではなく、他の PoS チェーンや PoS 的な構造を持つシステム(広義の PoS 系システム、以下単に「PoS ネットワーク」といいます。)に対してセキュリティを提供する。
(2) ステーキング報酬は、対象となるネットワークが設定する報酬(例：そのネットワークのネイティブトークン)で支払われる。
(3) 複数の PoS ネットワークに対して同時にステーキング(マルチステーク)することが可能であり、収益の向上が見込める一方、リスクも増加する。
(4) ステーキングの際に BTC の秘密鍵を移転する必要はなく、EOTS(Extractable One-Time Signatures)と呼ばれる署名技術を用いることで、トラストレスかつ非カストディアルに参加できる。

2 他の PoS ネットワークの安全性を担保するために BTC をステークするとは？

Babylon の最大の特徴の一つが、Bitcoin を使って「他の」ブロックチェーンのセキュリティを強化するという点です。

対象となるチェーンは、要件を満たすブロックチェーンであり、広義の PoS 系システム(独自の検証者セットを持つあらゆるネットワーク)が対象となり、現状では、ロールアップ、データ可用性チェーン、オラクルネットワークとの間でテスト統合およびパートナーシップが発表されています。

3 これまでの PoS チェーンのセキュリティとステーキング

これまでの PoS(Proof of Stake)チェーンでは、ネットワークの安全性はバリデーターが担保します。バリデーターは自ら(通常はそのチェーンのネイティブトークン、なお、delegated POS が可能な場合には第三者から委託を受けた資産も含みます。)をステークし、正しいトランザクションの検証とブロック生成を行います。不正行為が発覚すればステークした資産が一部没収(スラッシング)されるため、経済的なインセンティブがネットワークの信頼性を支える仕組みになっています。

しかし、PoS チェーンのステーキングに参加するためにはバリデーター(delegated POS では delegator も含みます。)が当該 PoS のトークンを購入する必要があり、新興 PoS チェーンや小規模チェーンでは、①そもそも当該トークンを持っている人が少ない(ステークのために購入するコスト、価格変動リスク)、②当該トークンを持っている人が分散されてい

ない、③これによりバリデーター数やステーキングに使われるトークンの数が少なくなり、セキュリティが不十分になる場合があるとされていました。例えば、バリデーターが少数に集中していることで、ネットワークの検閲リスクや停止リスクが高まり、攻撃への耐性が弱くなる可能性があります。

Babylon では、極めて大きな時価総額と流動性を有する BTC を活用し、BTC ホルダーによる署名を通じて PoS ネットワークのセキュリティに貢献する仕組みを提供することで、こうした課題に対する解決策の一つとなるとされています。

4　BTC を活用したセキュリティ強化

Babylon は、前述のとおり、従来の PoS ネットワークが抱えるセキュリティ上の課題に対し、ビットコイン(BTC)という外部資産を活用したセキュリティ提供の仕組みを構築しています。具体的には、BTC 保有者が自身の BTC を「経済的担保(economic security)」として提供することにより、PoS ネットワークに対して外部からのセキュリティ強化に寄与します。

ここで重要なのは、この「担保」としての BTC が PoS ネットワークに直接移転されるわけではないという点です。BTC は、BTC チェーン上の自己管理スクリプトに保持されたままであり、Babylon プロトコルを通じて暗号署名(デジタル証明)という形でステーキング意思を表明することで、担保提供が成立します。

この仕組みにより、BTC を第三者に預けたりロックアップしたりすることなく、非カストディアルかつトラストレスにセキュリティ提供を実現することが可能となっています。

このような外部的セキュリティの提供により、PoS ネットワークは、流動性と時価総額の高い BTC を活用して、ネイティブトークンだけに依存しないセキュリティ基盤の補強を行うことが可能になります。とくに、新興 PoS ネットワークにおいては、トークン分布の偏在やバリデーター数の少なさに起因する脆弱性を補完する手段として、有効性が期待されています。

5　報酬は PoS ネットワーク側のトークンで支払われる

Babylon を通じて BTC をステークすることで得られる報酬は、BTC ではなく、セキュリティを提供する対象となる PoS ネットワークが設定した報酬トークンです。

この報酬トークンは、通常その PoS ネットワークのネイティブトークン(例：ATOM、OSMO など)である場合が多く(但し、ネイティブトークンがない場合、ETH などが付与される想定の場合もあるようです)、PoS ネットワークが自身のネットワークのセキュリティ強化の対価として、BTC ステーカーに報酬を支払います。PoS ネットワーク側から見れば、自システムのトークンを利用して外部からセキュリティ資源(BTC)を調達できる仕組みであり、トークンのインフレやインセンティブ設計を通じて調整が可能です。

一方で、BTC ステーカー側にとっては、保有している BTC を動かすことなく、外部の

PoS ネットワークの報酬トークンを獲得できるというメリットがあります。特に BTC の長期保有者にとっては、新たな収益機会の一つとなり得ます。

報酬トークンが他の POS トークンであることのリスク

報酬トークンが他の POS トークンであることには幾つかのリスクが存在します。また、後述するように日本では暗号資産交換業者を通じてステークをする際、阻害要因になる可能性があります(後述 IV3)。

報酬が他の POS トークンであることによるリスク

- **報酬トークンの価格変動リスク**
  報酬として受け取る PoS ネットワークのトークンは、一般に BTC よりも時価総額や流動性が小さく、価格変動の影響を大きく受ける可能性がある。報酬額の名目値が大きくても、トークン価格が急落した場合、実質的な利回りが大きく低下する可能性がある。
- **報酬トークンの換金性・流動性リスク**
  得られる報酬トークンがニッチなチェーンのものである場合、市場での換金が難しかったり、スプレッドが大きく実効的な収益性が低くなる可能性がある。
- **報酬設計の継続性・安定性**
  PoS ネットワーク側が将来的に報酬設計を変更・縮小した場合、BTC ステーカーにとっての経済的魅力が損なわれる可能性がある。また、当該 POS ネットワークの運営が不安定な場合、報酬支払が適切に行われないリスクが存在する。

6　Babylon において秘密鍵を移転せずトラストレスでステーキングをする仕組

Babylon では、BTC ホルダーが自らの資産を「経済的担保」として PoS ネットワークのセキュリティに提供するにあたり、秘密鍵を第三者に移転することなく、自律的かつ非カストディアルな形で参加可能な設計となっています。この仕組みにより、従来のような資産移転やカストディへの信頼を前提としない「トラストレス」なステーキングが実現されます。

(1) 秘密鍵を移さないという意味

従来のステーキングや DeFi においては、資産を活用するために、以下のようないずれかの措置が必要でした。

- 資産(たとえば BTC)をラップトークン化し、別チェーン上で再利用(例：wBTC)
- カストディアンやスマートコントラクトに資産をロックし、担保とする

これらはいずれも、実質的に秘密鍵の制御を一時的に外部に委ねることになるため、「資産流出リスク」や「スマートコントラクトバグによる損失リスク」が存在します。

Babylon は、こうしたリスクを回避しつつ、署名ベースの仕組みによって、ステーカーが

BTC を保持したままセキュリティ参加を可能にする設計です。

(2) 技術的仕組み：ワンタイム署名(EOTS)によるステーキングの意思表明

Babylon では、Extractable One-Time Signatures(EOTS)と呼ばれる技術を用いることで、BTC ステーカーが自らの BTC 保有を証明すると同時に、PoS ネットワークへのセキュリティ提供に対する責任を明確に受け入れる仕組みが構築されています。

本仕組みにおける基本的なフローは以下のとおりです：

1	BTC ステーカーは、ファイナリティ・プロバイダーを選定し、ステーキング開始に必要なトランザクションデータを生成します。
2	このトランザクションには以下のような条件が含まれます： ①一定期間(例：3 日間)、当該 BTC を移動できない旨 ②その期間中に特定の条件が発生した場合には、BTC が指定された別のアドレス(通常はバーンアドレス)に送付される旨(スラッシング) ③一定期間経過前、かつスラッシングが起こっていない場合には、BTC ステーカーは自由にこのトランザクションを取り消す(解除する)ことができるという権利
3	②の「特定の条件」がスラッシングに該当し、たとえばファイナリティ・プロバイダーが不誠実な行動(例：二重署名)を行った場合に、BTC がバーンアドレスに強制送付される構造となります。
4	BTC ステーカーはこのトランザクションに対し、EOTS による一度限りの署名を行うことで、BTC 保有の証明およびステーキング意思の表明を完了します。

この設計により、PoS ネットワーク側は、BTC という流動性の高い外部資産に裏付けられたセキュリティ保証を受け取ることができ、さらに Babylon プロトコル上でスラッシング等の不正検出とペナルティ実行まで一貫して完結できるフレームワークが実現されています。

署名のやり方(出典：Babylon の Litepaper https://docs.babylonlabs.io/papers/btc_staking_litepaper%28EN%29.pdf?utm_source=chatgpt.com)

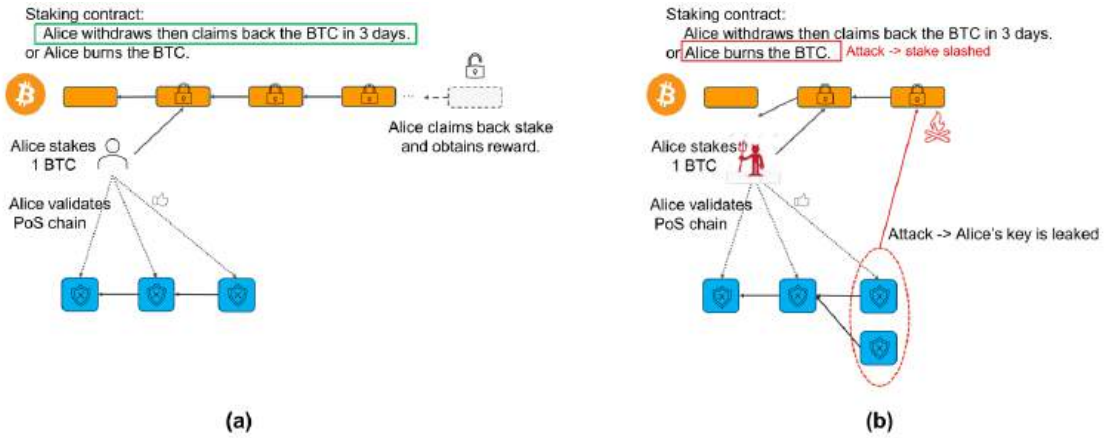


Figure 2: A Bitcoin staker's journey: (a) the happy path: Alice stakes, validates the PoS chain, requests unbonding, and unstakes in 3 days; (b) the unhappy path: Alice stakes, commits a safety offense to the PoS chain, and then her bitcoin got burned.

7　トラストレス性の意義とその限界

Babylon を利用した BTC ステーキングの仕組みは、以下の点において、トラストレスかつ非カストディアルな設計を特徴としています：

- 資産である BTC は、ユーザー自身の自己管理スクリプト上に保持されたままで、ステーキングに参加できること
- 中央集権的な第三者やスマートコントラクトに依存することなく、署名(デジタル証明)のみで担保提供の意思を表明できること
- この署名を通じてセキュリティ提供に参加し、報酬を得ることができること

このように、信頼を要する対象を最小限に抑えた構造は、ビットコインが本来的に志向する非トラスト・分散的原則とも整合的です。

もっとも、完全な「ゼロ信頼(trustless)」というわけではなく、後述する Babylon Genesis Chain が、署名の検証やスラッシングの実行、報酬処理などを担っている点には留意が必要です。

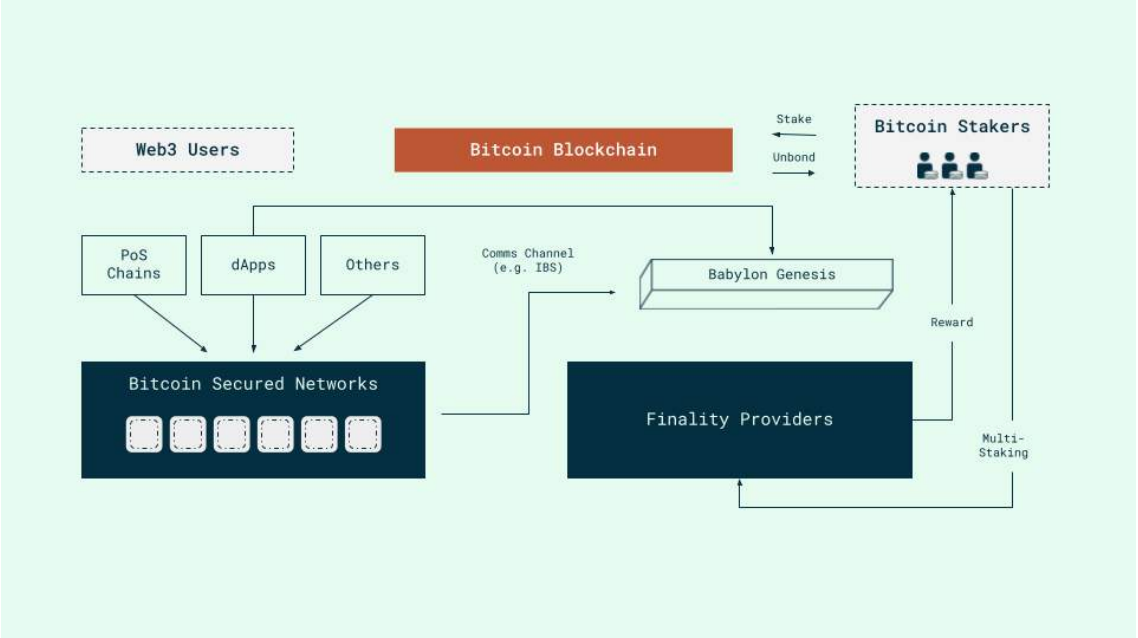
すなわち、BTC を直接預けることはないとはいえ、Babylon Genesis Chain を含む Babylon プロトコル全体の正当な運用と正確な実装に対する一定の信頼(protocol trust)が前提となっている点は理解しておく必要があります。

III. に関する重要なエンティティー

Babylon エコシステムに関連する登場人物は多岐に渡りますが、主要な登場人物としては下記のような者がいます。

1　Babylon に関する重要なエンティティー

図：Babylon Overview (出典：Babylon.docs https://docs.babylonlabs.io/guides/overview/)



(1) Bitcoin Secured Networks(BSNs)

- **概要：**

Babylon を介して Bitcoin の経済的セキュリティを導入し、自らの PoS ネットワークの安全性を強化しているネットワーク(チェーン)群を指します。

- **役割：**

PoS ネットワークは、バリデーターの分散性・経済的担保力の不足など、初期段階でセキュリティが脆弱になりやすいという課題を抱えることが少なくありません。BSNs はその補完手段として、Babylon 経由で外部から BTC を担保として導入し、以下のような目的を果たします。

1. BTC による追加的セキュリティの導入

BTC という高流動性・高信頼性の外部資産を活用し、ネットワーク攻撃に対する耐性を高めます(現在は double sign 二重署名に対処)。

2. ファイナリティの強化

Babylon のファイナリティ・プロバイダーによる署名に基づき、自システムのブロック

に対する「外部的な確定性(finality)」を得ることができます。

3. 報酬設計を通じた BTC ステーカーの誘致

BSNs は自らのトークンやステーブルコインなどを活用して、Babylon 経由の BTC ステーカーに報酬を提供し、セキュリティ強化のコストをインセンティブ設計で賄います。

- **対象例(想定)：**
  - 新興の Cosmos SDK ベースのアプリチェーン
  - 独自トークン価値が安定していない PoS プロジェクト
  - Ethereum の L2 チェーン
  - ゲームチェーン、DePIN ネットワーク、AI チェーン
  - その他、理論上は全ての PoS ネットワークに対応可とのこと

(2) ファイナリティ・プロバイダー(Finality Providers)

- **概要：**

Babylon がセキュリティを提供する PoS ネットワークのブロック確定(ファイナリティ)を観測し、署名を行う主体。

- **役割：**
  - ファイナリティ署名を作成・提出
  - 不正署名にはスラッシングリスクがあるため、誠実な行動が求められる
- **補足：**

ファイナリティ・プロバイダーは PoS ネットワークのブロックの最終性を確認し、Babylon チェーンにその情報を提供する役割を持つ点で、他のチェーンでいうバリデーターとは異なる役割を有します。しかしながら、署名を作成・提出し、その結果、報酬を得る、スラッシングリスクがある、という点ではある程度バリデーターと同種の役割を負うと思われます。

ファイナリティ・プロバイダーとバリデーターの比較

項目	ファイナリティ・プロバイダー(Babylon)	一般的な PoS チェーンのバリデーター
ブロック生成	❌ 行わない	✅ 実施する
ファイナリティ観測	✅ 実施する	❌ 通常は関与しない(ファイナリティは結果として形成)
署名	✅ ファイナリティに関する署名	✅ ブロックや投票に関する署名
スラッシング	✅ あり(不正署名)	✅ あり(二重署名・停止等)
報酬	✅ あり(署名に応じて)	✅ あり(ブロック生成・委任に応じて)

(3) ビットコインステーカー(Bitcoin Stakers)

- **役割：**

BTC を保有し、Babylon に署名(オフチェーン)を提供することで、他の PoS ネットワークのセキュリティに参加する。

- **報酬：**

ステーキング報酬(PoS ネットワークから支払われる)を BTC を担保に得る。

- **特徴：**

秘密鍵や BTC を他人に預けることなく参加可能。資産を非カストディアルに維持しつつ、ステーキング収益を得られる。

なお、BTC ステーカーはファイナリティ・プロバイダーに対して自身の BTC をステーク(委任)することができるが、この際も BTC 自体の移転や秘密鍵の共有は発生せず、非カストディアルな形で委任が完了する設計となっている。

(4) Babylon Genesis Chain(BSN の 1 つ)

- Babylon Genesis Chain は、Babylon プロトコルを稼働させるために構築された、Cosmos SDK ベースの PoS レイヤー1 ブロックチェーンです。
- Babylon Genesys Chain は、BSN の一つですが、Babylon 全体の中で、以下の中核的役割を担っています：

機能	説明
署名の検証	BTC ステーカーやファイナリティ・プロバイダーによる署名の受理・検証を行う
スラッシング処理	不正署名が発覚した場合にスラッシング(罰則)を執行
ファイナリティ記録	PoS ネットワーク上のブロックファイナリティを BTC 上で確定化する(タイムスタンピング)
クロスチェーンリレー	BSN(Bitcoin Secured Networks)へセキュリティ情報や署名をリレーする

- Babylon のファイナリティ・プロバイダーとして活動し、Babylon Genesis Chain にセキュリティを提供した場合、報酬としてネイティブトークンである「BABY」を得ることができます。

(5) リキッドステーキングプロトコル(Liquid Staking Protocol)※上記図には未記載

BTC 保有者に代わり、Babylon 経由での BTC ステーキングを効率化し、利便性や流動性を向上させるプロトコル。主にリキッドステーキングを中心としつつ、必要に応じて

リステーキング（再活用）も組み合わせるハイブリッドモデルが想定されます。
主な機能：

① オペレーションの簡素化 BTC 保有者自身が各 PoS ネットワークに対して署名やモニタリングを行うのは負担が大きいため、以下を代行： ステーキング先 PoS ネットワークの選定 EOTS 署名の自動生成・管理 報酬の受領・配分 ② リキッドステーキングトークン（LST）の発行と活用 ユーザーがステーキングした BTC に対して、プロトコルがステーキングポジションを裏付けとするリキッドステーキングトークン（例：stBTC）を発行。これによりステーク中でも資産の流動性を確保でき、DeFi などで二次利用が可能となります。 ③ リステーキング（Restaking）の補完的活用 同一の BTC を使った署名を、リスク管理を行いながら複数の PoS ネットワークに再活用（＝マルチステーキング）することで、収益性の最大化を図ります。

2　補足(Babylon エコシステムと Babylon Genesis Chain の関係)

Babylon エコシステム全体と、Babylon Genesis Chain との関係はやや複雑であるため、以下に整理します。

Babylon Genesis Chain は、Babylon エコシステムの中核的な役割を担う PoS ブロックチェーンですが、エコシステム全体と同一の概念ではありません。Babylon というプロトコル群は、より広範な枠組みを指しており、複数の Bitcoin Secured Networks(BSNs)を包含します。

ファイナリティ・プロバイダーとして Babylon に参加し、Babylon Genesis Chain にファイナリティを提供した場合、報酬としてネイティブトークンである「BABY」を得ることができます。

一方で、ファイナリティ・プロバイダーは、Babylon Genesis Chain に限らず、他の BSN(Bitcoin Secured Networks)にもファイナリティを提供可能であり、その場合には当該 BSN が設定する別の報酬トークンを受け取る仕組みとなっています。

なお、Babylon Genesis Chain には、BABY をステークしてネットワークのコンセンサス形成に参加する独自のバリデーターも存在します。これらのバリデーターも、ネットワークへの貢献に応じて BABY を報酬として得ることができます。

1　BABY トークンの獲得手段と役割

項目	内容

トークン名	BABY(Babylon Genesis Chain のネイティブトークン)
獲得手段①	Babylon Genesis Chain のバリデーターとして BABY をステークし、ブロック生成・検証に参加する
獲得手段②	ファイナリティ・プロバイダーとして、Babylon Genesis Chain に BTC を用いてファイナリティを提供する
用途①	バリデーターになるためのステーキング担保
用途②	ガバナンストークン(提案・投票への参加)
用途③	ネットワーク手数料(将来的に)
備考	他の BSN における報酬トークンは、BABY ではなく各 BSN の独自トークンとなる場合がある

2　ファイナリティ・プロバイダーとバリデーターの比較

項目	**ファイナリティ・プロバイダー**	**バリデーター(Babylon Genesis Chain)**
ステーク対象資産	BTC(非カストディアル)	BABY トークン(非カストディアル)
役割	PoS ネットワーク(BSN)へのファイナリティ提供(署名)	Babylon Genesis Chain のブロック生成・検証
対象チェーン	Babylon Genesis Chain および他の BSN	Babylon Genesis Chain 限定
報酬トークン	対象チェーンに応じて BABY または BSN の独自トークン	BABY トークン
不正時リスク	二重署名等で報酬無効・スラッシング(BTC の署名無効化)	二重署名や停止によるスラッシング(BABY ステーク減)
ステーキング方法	BTC 署名による意思表明（自己管理スクリプトで保有、委任も可能）	オンチェーンでの BABY トークンステーキング（自己管理型、委任も可能）

IV. Bitcoin ステーキングと日本法

以上のような前提知識をもとに、Babylon のような Bitcoin ステーキングサービスを提供する場合や利用する場合の法律論点を下記で検討します。

ただ、この点は結論としては、暗号資産法のカストディ規制の適用の有無、金商法のファンド規制の適用の有無を考える必要があります。

1　Babylon と暗号資産のカストディ規制

Babylon を通じた BTC ステーキングにおいて、Babylon に対して BTC のセキュリティを提供することが、暗号資産の「管理」すなわち「カストディ」に該当するのではないか、という論点が生じ得ます。

日本の資金決済法に基づくカストディ規制では、以下のパブリックコメント等から明らかなように、「秘密鍵を保持しているか否か」が重要な判断基準となっています。

> 令和元年資金決済法等改正に係る政令・内閣府令案等に対するパブリックコメント結果[19] 番
> 事業者が利用者の暗号資産を移転するために必要な秘密鍵を一切保有していない場合には、当該事業者は、主体的に利用者の暗号資産の移転を行い得る状態にないと考えられますので、基本的には、資金決済法第 2 条第 7 項第 4 号に規定する「他人のために暗号資産の管理をすること」に該当しないと考えられます。

この点、Babylon では、BTC を移転するための秘密鍵は、Babylon Genesis Chain やファイナリティ・プロバイダー等のいかなる主体にも移転されません。

具体的には、以下のような技術的構成となっています：

- BTC ステーカーは、ファイナリティ・プロバイダーを選定し、ステーキング開始に必要なトランザクションデータを生成
- そのトランザクションには、「①一定期間は動かさない、②スラッシングイベントが発生した場合にはバーンアドレスに送付」という条件付き送付内容(＝スラッシング予告)が含まれる
- BTC ステーカーはこのトランザクションに対し、EOTS による一度限りの署名を行うことで、BTC 保有の証明およびステーキング意思の表明を完了します。

このように、スラッシングの可能性を含んだ条件付きの署名は BTC ステーカー自身によって行われてはいるものの、これは条件付の署名であり、Babylon やその他の第三者が自由に当該資産をコントロールする構造にはなっていないと考えられます。

---

[1] https://www.fsa.go.jp/news/r1/sonota/20200403/01.pdf

そのように考えると、Babylon やファイナリティ・プロバイダーは、「暗号資産を移転するための秘密鍵を保有している」とは評価されず、資金決済法上のカストディ規制の対象には基本的に該当しないと考えて良いのではと思われます。

もっとも、Babylon 自体が秘密鍵を保持していないとしても、一部のリキッドステーキング事業者においては、ユーザーの秘密鍵を預かる形でサービスを提供している例も存在するようです。このような場合には、当該リキッドステーキング事業者が暗号資産のカストディ規制の対象となる可能性があるため、個別に法的整理・確認が必要となる点に留意が必要です。

2　Babylon と金商法規制

Babylon においては、BTC のセキュリティ提供を受け、その経済的担保により BTC ステーカーが報酬を受け取る一方、スラッシング等のペナルティリスクを負担する構造となっています。この点から、Babylon が日本法上のファンド(集団投資スキーム)に該当するかが問題となり得ます。

(1) 日本法における「ファンド(集団投資スキーム)」の定義

金融商品取引法(以下、金商法)第 2 条第 2 項第 5 号・第 6 号において、ファンドは概ね次のように定義されています。

(A) 対象となる権利形態(いずれか)

1. 組合契約
2. 匿名組合契約
3. 投資事業有限責任組合契約
4. 有限責任事業組合契約
5. 社団法人の社員権
6. その他これらに類する権利(外国の法令に基づくものを除く)

※上記 1～5 は例示列挙であり、形式を問わず広く「その他の権利」が含まれます。

(B) 投資スキームの内容(すべて満たす)

- 出資者が、出資または拠出した金銭またはこれに類する財産(政令上「暗号資産」も含む)を原資として
- 事業(出資対象事業)を行い
- その事業から生じた収益の配当または財産の分配を受ける権利を有すること

(C) 以下のいずれにも該当しないこと

- イ：出資者全員が事業に実質的に関与する場合(政令に基づく要件あり)
- ロ：出資者が出資額を超える分配を受けることがない場合(有限責任型)

(D) 外国法に基づく権利(外国ファンド)

(2) Babylon への適用の検討

Babylon は、上記(A)の「その他の権利」に該当する可能性があり、また(C)の例外事由にも該当しないと考えられます。

もっとも、(B)の要件との関係では、以下のような点から Babylon はファンドには該当しないと解されると思われます。

- BTC ステーカーによる「提供」は、出資や拠出というよりも、経済的セキュリティ(担保)の提供と位置づけられ、Babylon の運営主体に対する資金の移転ではない。
- ステーキングによって得られる報酬は、Babylon 自身の事業による収益の配当ではなく、PoS ネットワークから付与されるトークン報酬である点で、「出資対象事業に係る収益の配当」とは異なる。
- BTC ステーカーは、プロトコル上の署名に基づき自律的にステーク参加しているのみであり、特定の資産運用主体に資産を預けているわけではない。

これらの観点からは、Babylon における BTC のセキュリティ提供は、金商法上のファンドには該当しないと考えることが可能です。

(3) ファンド規制とファイナリティ・プロバイダーおよびリキッドステーキングプロトコル

Babylon においては、BTC ステーカーがファイナリティ・プロバイダーにステーキングを委任することが可能ですが、この場合も秘密鍵の移転は行われないため、ファンドの構造には該当しないと考えられます。

一方で、一部のリキッドステーキングプロトコルにおいては、ユーザーから秘密鍵を預かる形でサービスを提供している可能性があります。そのような場合には、当該リキッドステーキングプロトコルのスキームがファンドに該当するか、個別に秘密鍵の管理・拠出の有無などを踏まえて慎重に検討する必要があります。

V.　暗号資産取引所と Babylon ステーキング

本章では、日本の暗号資産交換業者が、ユーザーから預託された BTC を用いて Babylon チェーン上でステーキングを行う場合の法的・実務的な論点を検討します。

1　暗号資産交換業におけるステーキングの位置づけ

日本国内の多くの暗号資産交換業者が、ユーザー向けにステーキングサービスを提供しています。

当職らの理解では、少なくともユーザーにスラッシングリスク(損失リスク)を負担させない限り[2]、当該サービスは本業である「暗号資産の預託」(資金決済法第 2 条第 15 項第 4 号)と一体として実施可能と整理されていると認識しています。

この点は、Babylon を利用する場合でも同様であり、特段の変更を要するものではないと考えられます[3]。

2　ステーキングとコールドウォレット規制の整合性

暗号資産交換業者には、ユーザーから預託を受けた暗号資産について、自己の資産と分別したうえでコールドウォレットにて保管する義務が課されています(資金決済法第 60 条の 11 第 2 項、暗号資産交換業等に関する内閣府令第 27 条第 3 項第 1 号)。

PoS チェーンにおける一般的なステーキングでは、資産の移転にかかわる秘密鍵を移す必要はなく、バリデーターキーのみを用いる構成が多いため、当該保管義務との抵触はないと解されています。

---

[2] この点、スラッシングリスクを暗号資産交換業者が適切に管理できるのか、またそのリスクが業者の経営に与える影響はないのかといった点は、実務上重要な論点となります。通常、暗号資産交換業者がステーキングサービスを提供する際には、バリデーター(またはそれに相当する者)との間に業務委託契約が締結され、スラッシングリスクの負担に関する条項も規定されるのが一般的です。もっとも、バリデーター側がスラッシングに関するすべての損害に対して責任を負担できるとは限らず、財務的な体力に制約があるケースも多いのが実情です。さらに、保険などを通じたリスクヘッジにも限界があるため、交換業者としては、スラッシングによる損失が発生した場合の補償体制をどのように整備すべきかが課題となります。このように、ステーキングにおいて発生し得るスラッシングリスクを、ユーザー・交換業者・バリデーターのいずれがどの範囲で負担するのが妥当かについては、実務的にも検討が求められるポイントといえます。

なお、ユーザーが交換業者を介さずに、自らの判断で直接バリデーターを指定してステーキングを行う場合には、一般的にスラッシングリスクはユーザー自身が負担する構造になるものと考えられます。

[3] なお、ユーザーにスラッシングリスクを負担させる場合には、当該スキームが金融商品取引法上のファンド(集団投資スキーム)に該当する可能性がある点には留意が必要です。

もっとも、現時点でこの点について詳細な検討を行っているわけではなく、ユーザーからの預託＋委任契約が組み合わさった形態であり、委任契約に基づいて損失を負担させても、特にファンドではない等と整理する余地もあるかもしれません。

Babylon においてはバリデーターキーという概念は存在しませんが、Extractable One-Time Signatures(EOTS)と呼ばれる署名によってステーキングが実行され、秘密鍵は常に BTC ステーカー(今回の場合は交換業者)が保持しています。

したがって、交換業者が秘密鍵を移動・管理する構成にはなっておらず、コールドウォレット規制との矛盾は生じないと考えられます。

3　Babylon において発生するアルトコイン報酬の取扱い

Babylon ステーキングにおける実務的な論点の一つは、BTC をステーキングしているにもかかわらず、実際の報酬が PoS ネットワークのネイティブトークン(アルトコイン)で支払われることが多いという点です。

例えば、ETH をステーキングする場合、報酬としても ETH が支払われるため、すでに「取扱暗号資産」として届出済の交換業者では問題は生じません。

しかし、Babylon を介した BTC ステーキングでは、BABY やその他の PoS トークンといった“非取扱通貨”が報酬として発生する可能性があり、これが法務・運用上の対応を要するポイントとなると思われます。

このような状況に対する取引所の対応案は、以下のとおり整理されます。

(1) アルトコインを取引所がカストディし、ユーザーに付与する

この場合、取引所が当該アルトコインを自ら保有し、ユーザーに対して付与・管理を行うことになります。

しかし、当該アルトコインが資金決済法上の「取扱暗号資産」として届出されていない場合、法的にカストディを行うことはできません。

一部の主要トークン(例：BABY)については取扱通貨として届出する可能性もあり、また Babylon のパートナーとして想定される一部のトークンでは既に上場されているものもあるようですが(例：ATOM、SUI)、全ての報酬通貨について個別に届出を行うのは現実的とは言えません。

(2) アルトコインをユーザー自身のウォレットに送付する

この方法では、取引所は当該アルトコインのカストディを行わず、報酬としてのトークンをユーザーの自己管理ウォレットに直接送付するのみとなるため、取扱通貨の届出義務は生じないと考えられます。

もっとも、多くのユーザーに対して当該アルトコイン用のウォレット作成・管理を求めることは、UX やカスタマーサポートの観点から現実的とは言い難く、また送付に伴う取引コストやオペレーションリスクも無視できません。

(3) アルトコインを売却・交換し、BTC または円でユーザーに付与する

このスキームでは、取引所が報酬として受領したアルトコインを、DEX や海外事業者等で売却・交換し、その対価として得た BTC や円をユーザーに付与します。

この処理については、取引所が非取扱暗号資産の売買を行うこととなり、「暗号資産交換業」に該当するのではないかという懸念が生じます。

しかし、ユーザーとの契約において「ユーザーが BTC を取引所に預託し、取引所がステーキングの結果、ユーザーに報酬として BTC または円を付与する」ことが明確にされている場合おり、Babylon から得た報酬は単にその対価資金として用いられているにすぎないと解釈することも可能です。

このように構成されている限り、取引所が非取扱暗号資産を自己勘定で取得・処分しているに過ぎず、暗号資産交換業に該当するとは言い難いと考えられます。

(4) 結論

以上を踏まえると、現行法制のもとでは、取引所としては上記(3)のスキームを前提に実務を設計することが、最も現実的かつ実効的な対応策であると思われます。

もっとも、BSN 側にとっては、報酬トークンが継続的に売却されることによる売り圧力などの懸念もあると聞いており、制度としての持続可能性を含めた視点から検討を行う必要があると思われます。

謝辞

なお、本稿の作成にあたっては、Babylon ステーキングに精通する株式会社 Kudasai および株式会社 Next Finance Tech の皆様から貴重なご意見を賜ったほか、Babylon プロトコルの関係者の方々からも、非公式ながら有益な示唆を頂戴しました。

ただし、本稿に含まれる見解および誤りは、すべて筆者個人の責任に属するものであり、特定の事業者や団体の公式見解を示すものではありません。

留保事項

・本書の内容は関係当局の確認を経たものではなく、法令上、合理的に考えられる議論を記載したものにすぎません。また、当職らの現状の考えに過ぎず、当職らの考えにも変更がありえます。

・本稿は、ステーキング、Bitcoin ステーキング、Babylon、リキッドステーキング等の利用を推奨するものではありません。

・本書は Blog 用に纏めたものに過ぎません。具体的案件の法律アドバイスが必要な場合には各人の弁護士にご相談下さい。

以　上